REMARKS

Claims 1-9, 12-17, 19-21, 23, 25-41, and 45-50 are currently pending in the subject application and are presently under consideration. Claims 1, 7, 12, 15-17, 25, 26, 30-34, 36, 38-41, 49, and 50 have been amended as shown on pages 2-12 of the Reply. New claim 51 has been added.

Applicants' representative thanks Examiner Baum for the courtesies extended during the telephonic interview conducted on January 26, 2010. During the interview, the Examiner acknowledged a number of omissions in the Office Action, and clarified his reasoning behind several of the rejections therein. The Examiner also offered suggestions for claim amendments that he believes will better position the claims for allowance. The Examiner indicated that, if the amended claim set herein is still found to fall short of allowance, he will contact applicants' representative by phone to discuss additional amendments that will place the claims in condition for allowance.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1-9, 12-17, 19-21, 23, 25-41, and 45-50 Under 35 U.S.C. §103(a)

Claims 1-9, 12-17, 19-21, 23, 25-41, and 45-50 stand rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Swiler, *et al.* (US 7,013,395) in view of Townsend (U.S 6,374,358), and further in view of Godwin (US 2004/0059920). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Swiler, *et al.*, Townsend, and Godwin, individually or in combination, do not disclose or suggest all features of the subject claims.

> To reject claims in an application under § 103, an examiner must establish a prima facie case of obviousness. A prima facie case of obviousness is established by a showing of three basic criteria. First, there must be some apparent reason to combine the known elements in the fashion claimed by the patent at issue (*e.g.*, in the references themselves, interrelated teachings of multiple patents, the effects of demands known to the design community or present in the marketplace, or in the knowledge generally available to one of ordinary skill in the art). To facilitate review, this analysis should be made explicit. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. See MPEP § 706.02(j).

> See also KSR Int'l Co. v. Teleflex, Inc., 550 U.S. 398, 04-1350, slip op. at 14 (2007). The reasonable expectation of success must be found in the prior art and not based on applicant's disclosure. See In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)

The present application relates generally to network and automation device security in an industrial automation environment. According to one or more embodiments, a network-based security learning system (*e.g.*, a learning component) can be provided that monitors an automation network during a predetermined training period. During the training period, the learning component can monitor and learn activities or patterns such as the number of network requests to and from one or more assets, the type of requests, status or counter data, or substantially any data type or pattern that can be retrieved from the network or asset. After the training period, the learning component can monitor the automation network or assets for detected deviations from data patterns learned during the training period. If desired, a user interface can be provided, wherein one or more pattern thresholds can be adjusted. An alarm or automated event can then occur if a deviation is detected outside the threshold (see, *e.g.*, page 5, line 11 - page 6, line 5). In particular, amended independent claim 1 recites, *an interface component that generates a description of one or more industrial devices on a network, wherein the description includes at least a* ***learned pattern of network activity****...a user interface that accepts input* ***defining a pattern threshold****, the pattern threshold specifying an acceptable deviation from the learned access pattern; an analyzer component that* ***generates one or more security outputs if a current access pattern deviates from the learned access pattern in excess of the acceptable deviation****, the one or more security outputs including at least one output that alters the current access pattern.*

Swiler, *et al.* does not disclose or suggest at least these features. Swiler, *et al.* relates to an analysis tool that assesses potential security risks in a network. This analysis tool uses as input a database of common attacks broken into atomic steps, specific network configuration and topology information, and an attacker profile. The attack information is matched with the network configuration information and an attacker profile to create an attack graph. Graph algorithms are then applied to the attack graph to identify attack paths with the highest probability of success (see column 3, line 67 - column 4, line 11) . However, Swiler, *et al.* makes no determination as to whether a *current access pattern for a network deviates from a*

learned access pattern in excess of an acceptable deviation specified by a pattern threshold. Indeed, Swiler, et al. does not assess a network's current access pattern for any purpose, and therefore fails to contemplate comparing such an current access pattern with a learned access pattern.

Since Swiler, *et al.* fails to disclose determining whether *a current access pattern deviates from a learned access pattern in excess of an acceptable deviation*, it follows that the cited reference is also silent regarding generation of one or more security outputs that alter a current access pattern for the network. In this regard, it is noted that the above-described attack graph is employed for informational purposes only in order to assess a risk to network assets. Since the attack graph of Swiler, *et al.* is merely employed for informational purposes, the cited reference does not contemplate generating any type of security output, much less doing so based on whether a current access pattern deviates from a learned access pattern in excess of an acceptable deviation.

Townsend is also silent regarding these aspects. Townsend relates to a method selecting a security model for protecting an application from attack by unauthorized sources. To this end, a current countermeasure strength level and a recommended countermeasure strength level are determined for each of at least one countermeasure based on input data and security risk data. A security model including at least one countermeasure and a corresponding strength level is determined based on the current and the recommended strength levels (see column 2, lines 19-29). However, Townsend does not make a determination as to whether a *current access pattern for a network deviates from a learned access pattern*. Rather, the security model selection method of Townsend compiles business concerns, potential network attack types, and possible countermeasures, and uses this data to analyze each possible countermeasure with respect to each attack type for cost and effectiveness. None of this data entails an analysis of a *current or learned access pattern* for the network, and consequently the cited reference makes no determination regarding whether a *current access pattern for a network deviates from a learned access pattern*.

Moreover, like Swiler, *et al.*, Townsend does not generate a security output that can alter the current access pattern, or perform a direct action of any kind on a system under analysis. With regard to outputs, Townsend merely generates a written report of the above-described assessment that includes a recommendation for countermeasure implementation (see column 8,

lines 1-13). Townsend therefore fails to remedy the deficiencies of Swiler, *et al.* with regard to *generating one or more security outputs if a current access pattern deviates from the learned access pattern in excess of the acceptable deviation*, wherein *the one or more security outputs includes at least one output that alters the current access pattern.*

Godwin does not cure the above deficiencies. Godwin relates to a tool for checking storage management system security settings. This tool accesses one or more security parameters, compares them to security policies, rules, and allowable values, and reports noncompliant settings *via* a user-readable report. According to Godwin, a set of automatic correction rules may also be employed to automatically modify noncompliant settings to bring them into compliance (see Abstract). However, these parameter checks do not involve any manner of assessment on network access patterns generally. Rather, Godwin merely performs a check on each storage security parameter to ensure the parameter is within a compliant range. As such, Godwin fails to remedy the shortcomings of the other cited references with regard to an analyzer component that generates one or more security outputs *if a current access pattern deviates from the learned access pattern in excess of an acceptable deviation, the one or more security outputs including at least one output that alters the current access pattern.*

Similarly, amended independent claim 12 recites, ***monitoring access to the one or more industrial automation devices for a predetermined training period to learn at least one access pattern****; defining a pattern threshold specifying an acceptable deviation from the at least one access pattern; and* ***performing at least one automated security event if a current access pattern deviates from the at least one access pattern in excess of the acceptable deviation after the training period****, wherein performing the at least one automated security event includes at least altering a network traffic pattern associated with the one or more industrial automation devices.* None of Swiler, *et al.*, Townsend, or Godwin disclose or suggest performing an automated security event if a current access pattern deviates from a learned access pattern in access of an acceptable deviation, as discussed *supra.* The cited references also fail to disclose learning this learned accesses pattern by *monitoring access to one or more industrial automation devices for a predetermined training period.*

Likewise, amended independent claim 16 recites, *means for learning at least one access pattern for accessing the one or more industrial devices;...means for defining a pattern threshold that specifies an acceptable deviation from the at least one access pattern learned by the means*

for learning; means for ***automatically detecting that a current access pattern deviates from the at least one access pattern in excess of the acceptable deviation****; and means for* ***performing an automated action that alters the current access pattern in response to the detecting***. As discussed above, the cited references are silent regarding these features.

Also, amended independent claim 17 recites, *a component that automatically alters at least one traffic pattern on the network in response to detecting that a current pattern of access on the network has deviated from a learned pattern of access in excess of a defined pattern threshold.* Swiler, *et al.*, Townsend, and Godwin are silent regarding these aspects, as noted previously.

Amended independent claim 26 recites, *monitoring a network comprising one or more industrial automation devices to learn at least one access pattern; defining a pattern threshold that specifies an allowable deviation from the at least one access pattern; [and]* ***performing an automated security procedure that adjusts at least one security parameter on the one or more industrial automation devices if the scanning determines that a current access pattern deviates from the at least one access pattern in excess of the allowable deviation***, and as noted *supra*, the cited references fail to disclose or suggest these features.

Also, amended independent claim 30 recites, *means for* ***monitoring an industrial network comprising one or more industrial automation devices to learn at least one access pattern****; means for defining a pattern threshold that specifies an allowable deviation from the at least one access pattern;...means for* ***initiating a security procedure that adjusts at least one security parameter in the one or more industrial automation devices if the means for scanning identifies that a current access pattern deviates from the at least one access pattern in excess of the allowable deviation.*** As discussed above, none of Swiler, *et al.*, Townsend, or Godwin disclose or suggest these aspects.

Amended independent claim 31 recites, *a learning component that* ***monitors and learns industrial network access activities during a training period to determine at least one network access pattern****; a user interface that accepts first input specifying an acceptable deviation from the at least one network access pattern; and a detection component that* ***automatically triggers a security event based upon detected deviations of subsequent industrial network access activities in excess of the acceptable deviation after the training period****, wherein the security event includes adjusting at least one security parameter that alters a network traffic pattern*

associated with the industrial automation environment. The cited references are silent with regard to these learning and security aspects, as discussed *supra*.

Likewise, amended independent claim 39 recites, *monitoring a network of industrial devices for a predetermined time; automatically* ***learning at least one data transfer pattern of the network of industrial devices during the predetermined time****; defining a pattern threshold specifying an acceptable deviation from the at least one data transfer pattern; and* ***generating an alarm and altering network activity to adjust a current data transfer pattern if the current data transfer pattern is determined to be outside of the pattern threshold with respect to the at least one data transfer pattern***, and as discussed above, Swiler, *et al.*, Townsend, and Godwin fail to disclose or suggest at least these features.

Amended independent claim 41 recites, *means for* ***learning access patterns*** *with respect to at least one industrial automation device on the network; means for defining a pattern threshold specifying an acceptable deviation from at least one stored access pattern; and means for* ***generating a security event that disables network requests from at least one outside network upon determining that the access patterns learned by the means for learning are out of tolerance with the at least one stored access pattern by more than the acceptable deviation*** The cited references are silent regarding at least these features, as discussed *supra*. Furthermore, none of the cited references disclose or suggest *generation of a security event that disables network requests from at least one outside network*. In this regard, neither Swiler, *et al.* nor Townsend generate any type of output that effects a change to network behavior or activity, but rather only generate informational outputs in the form of security recommendations based on an analysis of system characteristics. Godwin merely discusses adjustment of security parameters when those parameters are found to be outside a specified allowable range, but is silent with regard to disabling network requests from an outside network.

Amended claim 49 recites, *the analyzer component further performs an automated action that disables network requests from at least one outside network upon detecting a deviation of the current access pattern from the learned pattern of network activity in excess of the acceptable deviation*. As already discussed, the cited references fail to disclose both an automated action that disables network requests from at least one outside network, and detection of a deviation of a current access pattern from a learned access pattern in excess of an acceptable deviation.

In view of at least the foregoing, it is respectfully submitted that Swiler, *et al.*, Townsend, and Godwin, individually or in combination, do not disclose or suggest all aspects of amended independent claims 1, 12, 16, 17, 26, 30, 31, 39, and 41 (and all claims depending there from), and as such fail to render obvious the present application. It is therefore requested that this rejection be withdrawn.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [ALBRP303USC].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

TUROCY & WATSON, LLP

/Brian Steed/
Brian Steed
Reg. No. 64,095

TUROCY & WATSON, LLP
57TH Floor, Key Tower
127 Public Square
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731